

To: Riverside County PCP& Specialists
From: Provider Relations
Date: October 30, 2026
Subject: **RCMA Action Alert: Phone Scams & Fraudulent Payment Change Requests**

Riverside County Medical Association (RCMA) has received reports of scams targeting physicians and their practices, including callers impersonating government officials and documents requesting changes to banking or payment information.

Phone calls impersonating government agencies

Physicians are receiving fraudulent calls from individuals claiming to represent the Drug Enforcement Administration (DEA), Medical Board of California, a District Attorney's Office, or the Department of Justice. Callers may request information about the physician or practice, claim money is owed, or threaten arrest or license suspension unless payment is made immediately.

Scammers may know your professional credentials and manipulate caller ID to display an agency's actual phone number.

If you receive a suspicious call:

- **Do not disclose or confirm sensitive information**, including banking details, Social Security numbers, passwords, verification codes, or patient information.
- **Do not send money** in response to threats or demands for immediate payment.
- **Hang up and independently contact the agency** using a number from its official website. Do not use a callback number supplied by the caller.

The DEA and Medical Board of California warn that their personnel will not telephone physicians demanding payment. See the official [DEA warning](#) and [California Department of Consumer Affairs alert](#).

Please share this alert with your practice administrator, billing team, accounting personnel, and staff who answer phones.

Suspicious W-9s and requests to change bank accounts

RCMA is also hearing reports of W-9 forms and accompanying notices being used to communicate supposed changes to bank accounts or payment instructions. These requests may appear to come from a familiar vendor, physician, practice, or other business partner.

A W-9 or an official-looking document alone should never be accepted as verification of a banking change. Fraudulent requests can arrive through convincing emails or compromised legitimate accounts.

Before changing any banking details, mailing address for payments, ACH instructions, or wire transfer information:

- **Pause the change and any affected payment until the request is independently verified.** Do not let urgency override your normal procedures.
- **Call a known, authorized contact using a previously verified phone number already in your records.** Do not use a new number provided in the email, W-9, attachment, or change notice.
- **Confirm both the request and the exact new payment instructions.** Replying to the same email thread is not sufficient verification.
- **Require a second authorized staff member to review and approve the change,** and document how it was verified before updating your records or releasing funds.

These steps align with the [FBI's guidance on preventing payment diversion scams](#).

If you suspect fraud or have already responded

Preserve emails, attachments, voicemails, and payment records.

If money has been sent, contact your bank or payment provider immediately to request assistance stopping or recalling the payment. Report suspected fraud to the [FBI's Internet Crime Complaint Center](#) or the [Federal Trade Commission](#).

If personal identifying information was disclosed, visit [IdentityTheft.gov](#) for recovery guidance.

When in doubt, stop and verify through a trusted, independently established contact before sharing information, changing payment instructions, or sending money.

If you have any questions, please contact the IEHP Provider Call Center at (909) 890-2054, (866) 223-4347 or email ProviderServices@iehp.org

All IEHP communications can be found at: www.providerservices.iehp.org > News and Updates > Notices